PROJECT INITIATION / Phase 2

Title: Network Intrusion Protection: IPS and IDS Overview

Student : Abdaullah Mohammad Mustafa Abughallous / 3220603043

Instructor: Dr.Firas Alzobi

Executive Summary

This report documents the successful implementation of an Intrusion Detection System (IDS) using Snort 3 on Kali Linux.
The project demonstrates real-time network traffic inspection , custom rule creation , and threat detection capabilities in a virtualized environment.
The system was tested against multiple attack vectors including ICMP ping floods, port scans, and network reconnaissance attempts with successful detection and logging of all identified threats.

Detection Rules

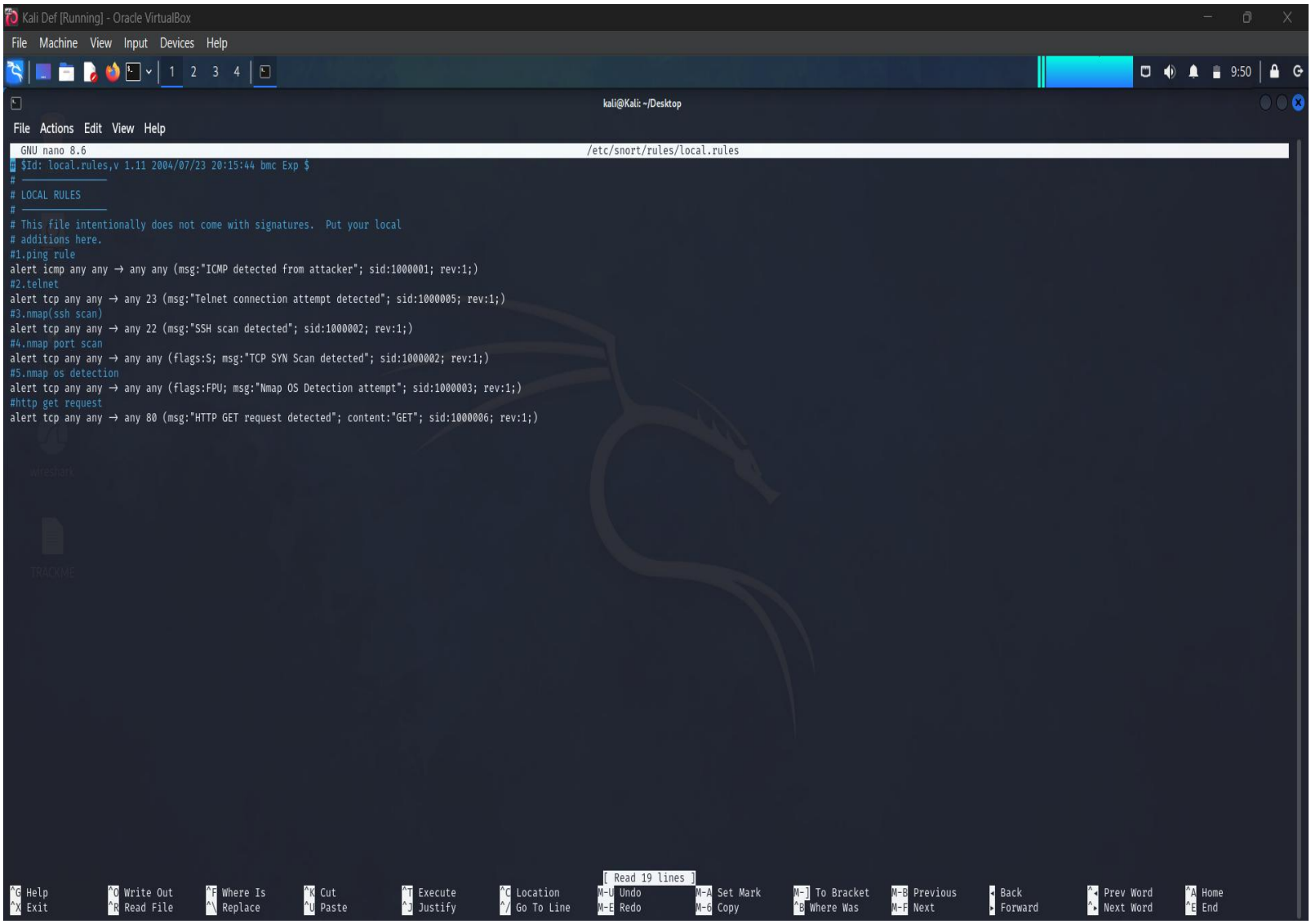
Snort rules follow a specific syntax:

alert protocol src_ip src_port -> dst_ip dst_port

(msg:"Description"; sid:unique_id; rev:version; content:"pattern";)

Components:

- `alert` → Action (alert/drop/reject)
- `protocol` → TCP, UDP, ICMP, IP
- `src_ip/src_port` → Source (any = all)
- `dst_ip/dst_port` → Destination
- `msg` → Alert message
- `sid` → Unique rule ID



-

Detection Summary Table

Attack Type	Rule SID	Detection Status	Alerts Generated
ICMP Ping	1000001	✓ Detected	+20 alerts
TCP SYN Scan	1000002	✓ Detected	~1000 alerts
Nmap OS Detection	1000003	✓ Detected	Multiple alerts

Attack Type	Rule SID	Detection Status	Alerts Generated
SSH Attempt	1000005	✓ Detected	Multiple attempts
Telnet Attempt	1000006	PARTIAL	Connection refused
HTTP Traffic	1000007	PARTIAL	Web requests

Conclusion

This project successfully demonstrated the implementation and operation of an Intrusion Detection System using Snort 3 on Kali Linux. The system effectively detected multiple attack vectors including network reconnaissance, port scanning, and service enumeration attempts.

Key Achievements:

- ✓ Installed and configured Snort 3 in passive IDS mode
- ✓ Created custom detection rules for 5+ attack types
- ✓ Successfully detected and logged all test attacks
- ✓ Generated comprehensive alert logs
- ✓ Identified and resolved technical challenges
- ✓ Established foundation for IPS implementation

The platform is now ready for transition to active Intrusion Prevention mode where detected attacks will be blocked in real-time rather than merely logged and alerted. This project provides valuable hands-on experience with network security tools and concepts essential for professional cybersecurity practice.

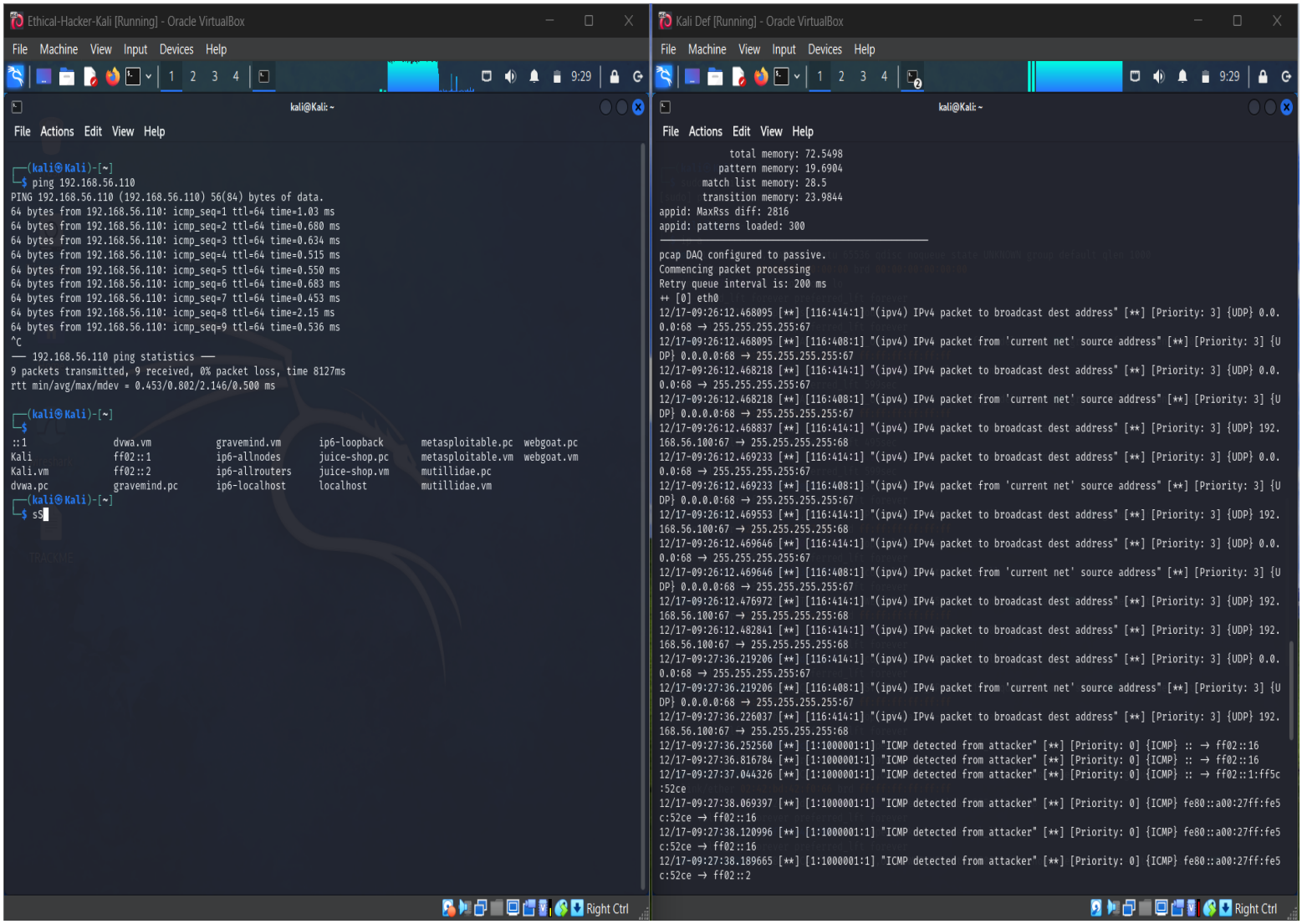
SCREENSHOT FOR TESTING

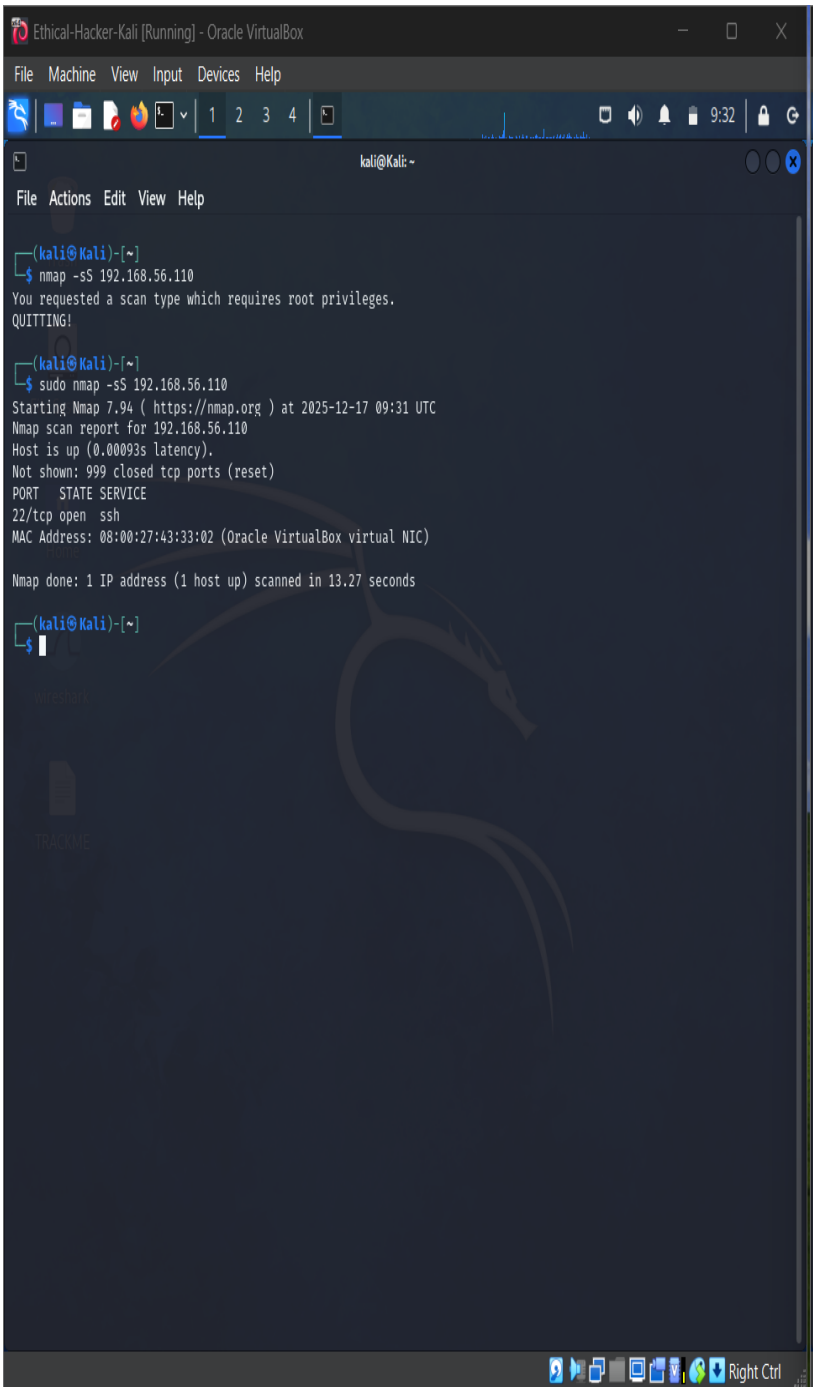
sudo snort -c /etc/snort/snort.lua -T

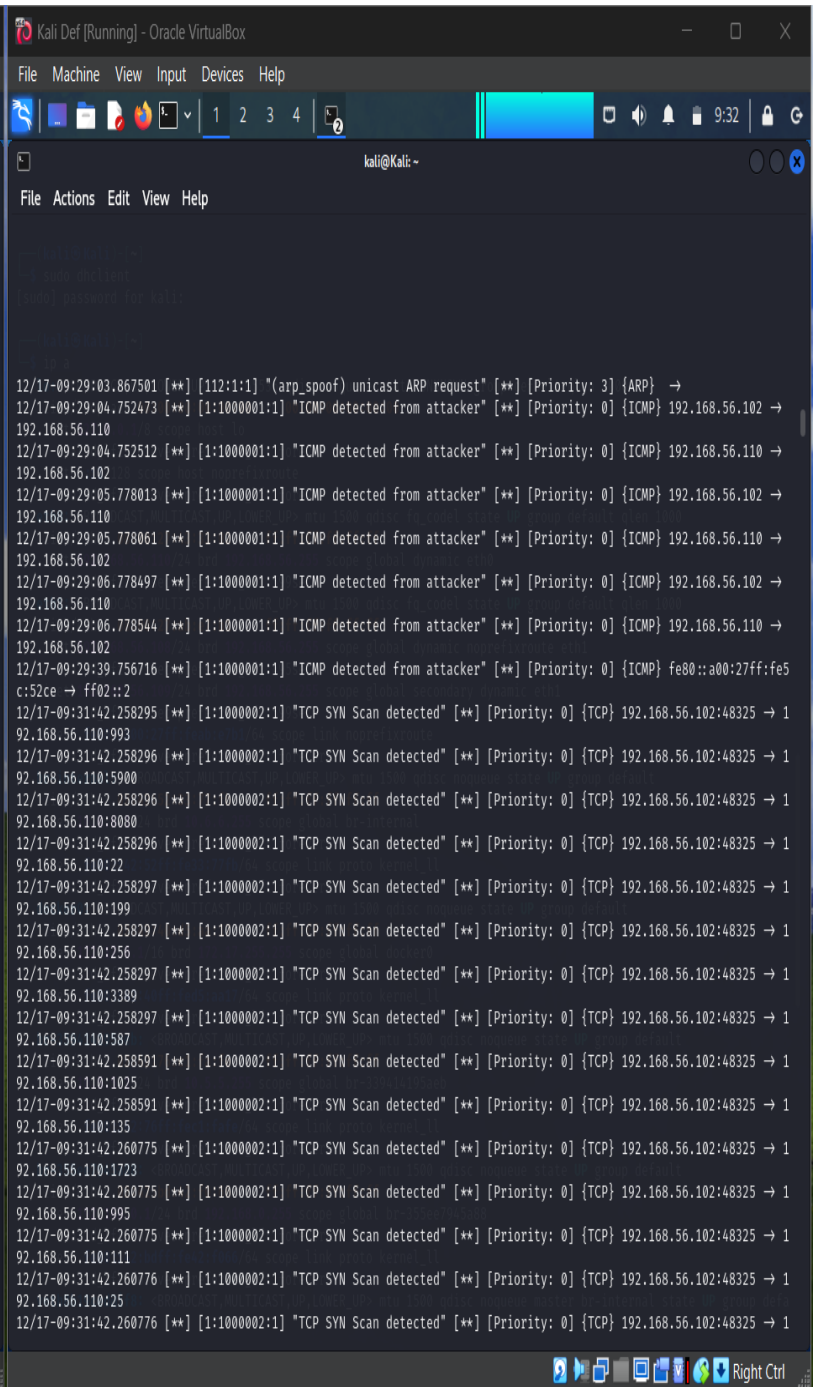
Run IDS

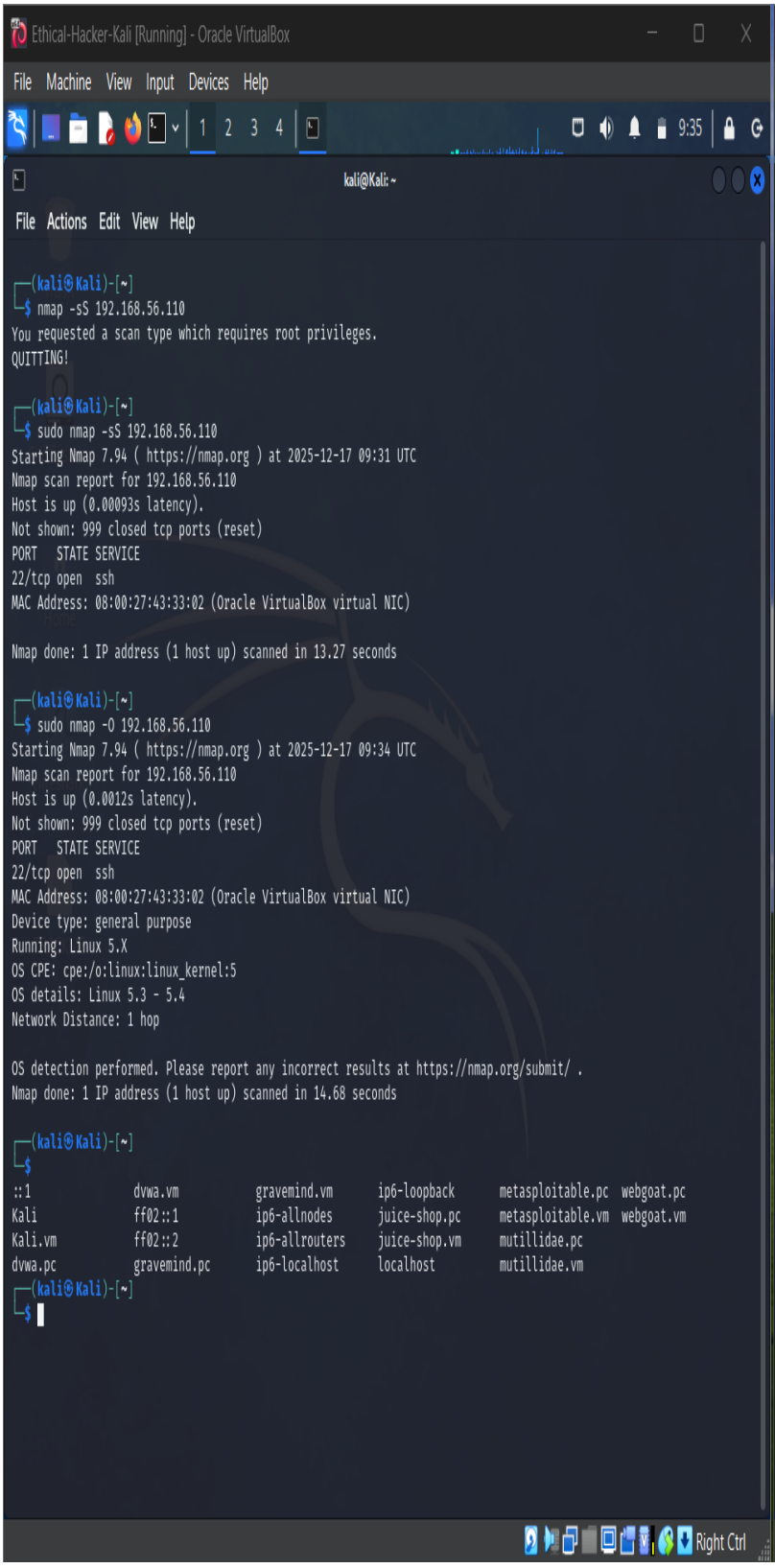
sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Test connectivity(PING) , NMAP(SYN,OS) , SSH , TELNET , HTTP

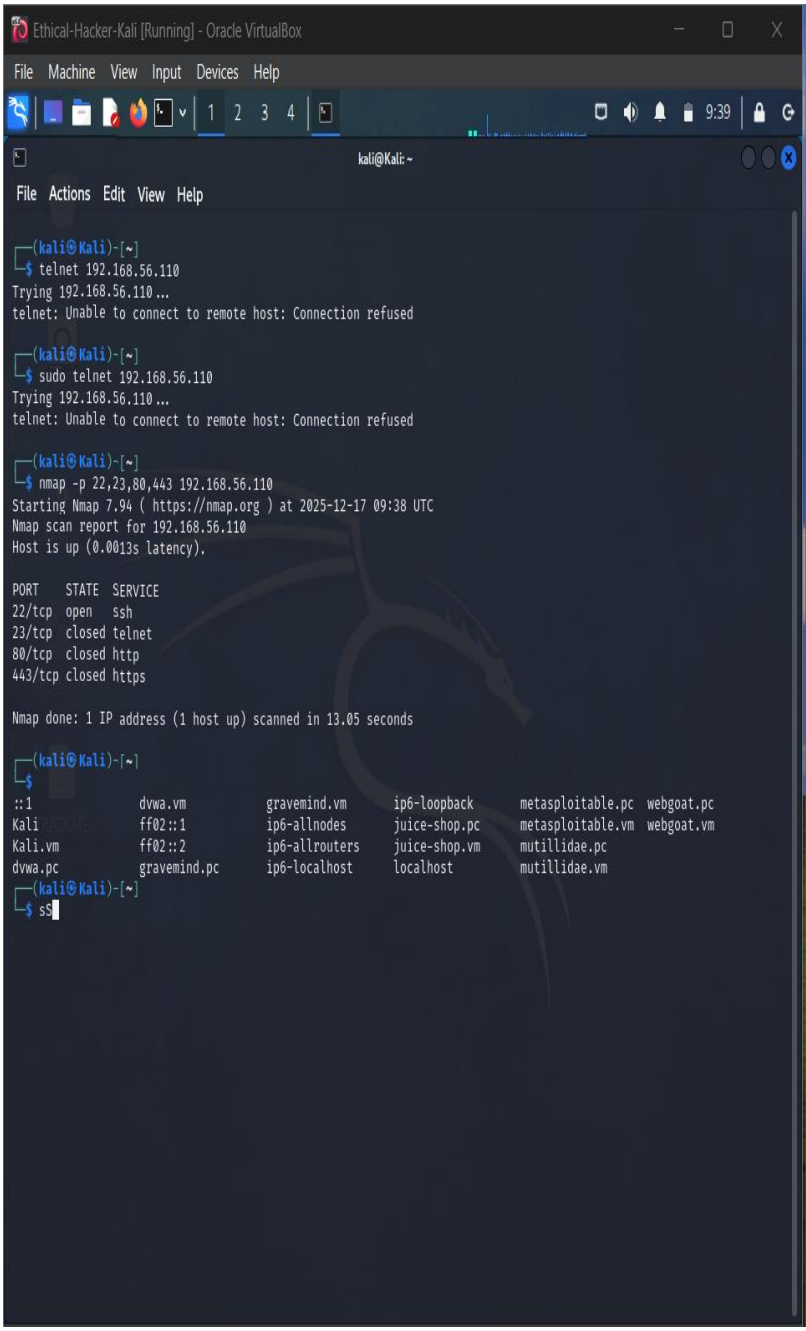



Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:32
kali@Kali: ~
File Actions Edit View Help
┌──(kali㉿Kali)-[~]
└─$ nmap -sS 192.168.56.110
You requested a scan type which requires root privileges.
QUITTING!
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -sS 192.168.56.110
Starting Nmap 7.94 (https://nmap.org) at 2025-12-17 09:31 UTC
Nmap scan report for 192.168.56.110
Host is up (0.00093s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 08:00:27:43:33:02 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
┌──(kali㉿Kali)-[~]
└─$
Right Ctrl

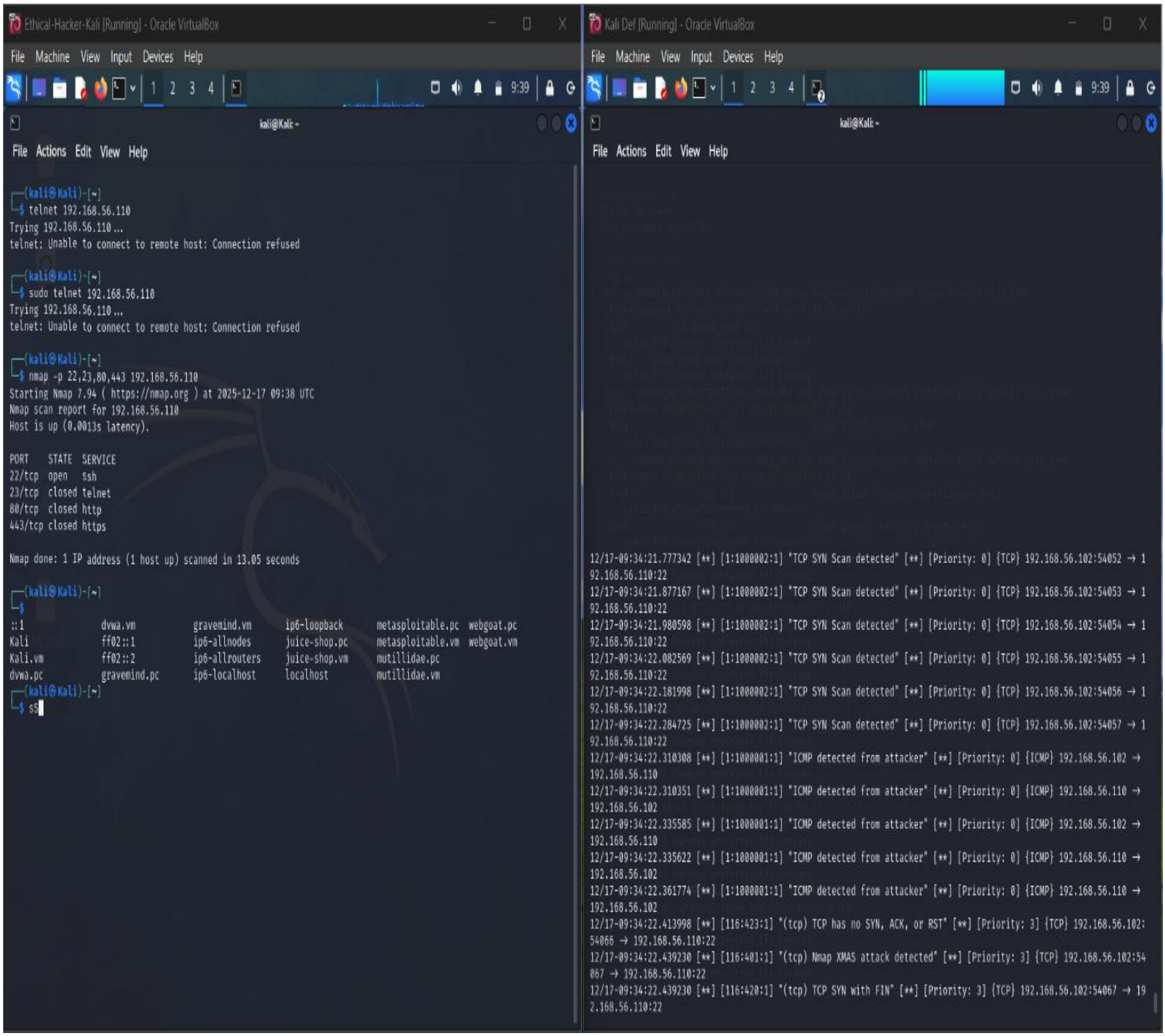

Kali Def [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:32
kali@Kali: ~
File Actions Edit View Help
12/17-09:29:03.867501 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/17-09:29:04.752473 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.56.110
12/17-09:29:04.752512 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:29:05.778013 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.56.110
12/17-09:29:05.778061 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:29:06.778497 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.56.110
12/17-09:29:06.778544 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:29:39.756716 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} fe80::a00:27ff:fe5c:52ce → ff02::2
12/17-09:31:42.258295 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:993
12/17-09:31:42.258296 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:5900
12/17-09:31:42.258296 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:8080
12/17-09:31:42.258296 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:22
12/17-09:31:42.258297 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:199
12/17-09:31:42.258297 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:256
12/17-09:31:42.258297 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:3389
12/17-09:31:42.258297 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:587
12/17-09:31:42.258591 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:1025
12/17-09:31:42.258591 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:135
12/17-09:31:42.260775 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:1723
12/17-09:31:42.260775 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:995
12/17-09:31:42.260775 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:111
12/17-09:31:42.260776 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:25
12/17-09:31:42.260776 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 1
Right Ctrl


Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:35
kali@Kali: ~
File Actions Edit View Help
┌──(kali㉿Kali)-[~]
└─$ nmap -sS 192.168.56.110
You requested a scan type which requires root privileges.
QUITTING!
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -sS 192.168.56.110
Starting Nmap 7.94 (https://nmap.org) at 2025-12-17 09:31 UTC
Nmap scan report for 192.168.56.110
Host is up (0.00093s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 08:00:27:43:33:02 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -O 192.168.56.110
Starting Nmap 7.94 (https://nmap.org) at 2025-12-17 09:34 UTC
Nmap scan report for 192.168.56.110
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 08:00:27:43:33:02 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.3 - 5.4
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds
┌──(kali㉿Kali)-[~]
└─$
::1 dvwa.vm gravemind.vm ip6-loopback metasploitable.pc webgoat.pc
Kali ff02::1 ip6-allnodes juice-shop.pc metasploitable.vm webgoat.vm
Kali.vm ff02::2 ip6-allrouters juice-shop.vm mutillidae.pc
dvwa.pc gravemind.pc ip6-localhost localhost mutillidae.vm
┌──(kali㉿Kali)-[~]
└─$
Right Ctrl


Kali Def [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:35
kali@Kali: ~
File Actions Edit View Help
12/17-09:31:45.392518 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} fe80::a00:27ff:fe5c:52ce → ff02::2
12/17-09:31:47.451517 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/17-09:34:13.884170 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:3306
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:5900
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:199
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:587
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:139
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:993
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:1723
12/17-09:34:21.572013 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:445
12/17-09:34:21.572217 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:443
12/17-09:34:21.572218 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:111
12/17-09:34:21.574713 [**] [1:1000005:1] "Telnet connection attempt detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:23
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:23
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:53
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:995
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:256
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:554
12/17-09:34:21.574713 [**] [122:1:1] "(port_scan) TCP portscan" [**] [Priority: 3] {TCP} 192.168.56.102:60838 → 192.168.56.110:554
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:113
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:110
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:25
12/17-09:34:21.575341 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:80
12/17-09:34:21.575341 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:3389
Right Ctrl


Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:39
kali@Kali: ~
File Actions Edit View Help
┌──(kali㉿Kali)-[~]
└─$ telnet 192.168.56.110
Trying 192.168.56.110 ...
telnet: Unable to connect to remote host: Connection refused
┌──(kali㉿Kali)-[~]
└─$ sudo telnet 192.168.56.110
Trying 192.168.56.110 ...
telnet: Unable to connect to remote host: Connection refused
┌──(kali㉿Kali)-[~]
└─$ nmap -p 22,23,80,443 192.168.56.110
Starting Nmap 7.94 (https://nmap.org) at 2025-12-17 09:38 UTC
Nmap scan report for 192.168.56.110
Host is up (0.0013s latency).
PORT STATE SERVICE
22/tcp open ssh
23/tcp closed telnet
80/tcp closed http
443/tcp closed https
Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
┌──(kali㉿Kali)-[~]
└─$
::1 dvwa.vm gravemind.vm ip6-loopback metasploitable.pc webgoat.pc
Kali ff02::1 ip6-allnodes juice-shop.pc metasploitable.vm webgoat.vm
Kali.vm ff02::2 ip6-allrouters juice-shop.vm mutillidae.pc
dvwa.pc gravemind.pc ip6-localhost localhost mutillidae.vm
┌──(kali㉿Kali)-[~]
└─$ s


Kali Def [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:39
kali@Kali: ~
File Actions Edit View Help
92.168.56.110:1
12/17-09:34:22.543592 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54071 → 192.168.56.110:1
12/17-09:34:22.543592 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54071 → 192.168.56.110:1
12/17-09:34:22.543592 [**] [116:422:1] "(tcp) TCP PDU missing ack for established session" [**] [Priority: 3] {TCP} 192.168.56.102:54071 → 192.168.56.110:1
12/17-09:34:22.569822 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54066 → 192.168.56.110:22
12/17-09:34:22.596583 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.596583 [**] [116:420:1] "(tcp) TCP SYN with FIN" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.596583 [**] [116:422:1] "(tcp) TCP PDU missing ack for established session" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.672422 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54066 → 192.168.56.110:22
12/17-09:34:22.696637 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.696637 [**] [116:420:1] "(tcp) TCP SYN with FIN" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.696637 [**] [116:422:1] "(tcp) TCP PDU missing ack for established session" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.772008 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54066 → 192.168.56.110:22
12/17-09:34:22.797771 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.797771 [**] [116:420:1] "(tcp) TCP SYN with FIN" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.797771 [**] [116:422:1] "(tcp) TCP PDU missing ack for established session" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:26.683587 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/17-09:35:53.223120 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} fe80::a00:27ff:fe5c:52ce → ff02::2
12/17-09:36:11.504786 [**] [1:1000005:1] "Telnet connection attempt detected" [**] [Priority: 0] {TCP} 192.168.56.102:36634 → 192.168.56.110:23
12/17-09:36:11.504786 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:36634 → 192.168.56.110:23
12/17-09:36:16.507890 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/17-09:36:16.624331 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/17-09:36:18.289713 [**] [1:1000005:1] "Telnet connection attempt detected" [**] [Priority: 0] {TCP} 192.168.56.102:36650 → 192.168.56.110:23
12/17-09:36:18.289713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:36650 → 192.168.56.110:23
12/17-09:38:31.923792 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:51854 → 192.168.56.110:80
12/17-09:38:31.923793 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:45844 → 192.168.56.110:443
12/17-09:38:37.051690 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/17-09:38:37.169761 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →


Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
(kali㉿Kali)-[~]
$ telnet 192.168.56.110
Trying 192.168.56.110 ...
telnet: Unable to connect to remote host: Connection refused
(kali㉿Kali)-[~]
$ sudo telnet 192.168.56.110
Trying 192.168.56.110 ...
telnet: Unable to connect to remote host: Connection refused
(kali㉿Kali)-[~]
$ nmap -p 22,23,80,443 192.168.56.110
Starting Nmap 7.94 (https://nmap.org) at 2025-12-17 09:38 UTC
Nmap scan report for 192.168.56.110
Host is up (0.0013s latency).
PORT STATE SERVICE
22/tcp open ssh
23/tcp closed telnet
80/tcp closed http
443/tcp closed https
Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
(kali㉿Kali)-[~]
$
::1 dvwa.vm gravemind.vm ip6-loopback metasploitable.pc webgoat.pc
Kali ff02::1 ip6-allnodes juice-shop.pc metasploitable.vm webgoat.vm
Kali.vm ff02::2 ip6-allrouters juice-shop.vm mutillidae.pc
dvwa.pc gravemind.pc ip6-localhost localhost mutillidae.vm
(kali㉿Kali)-[~]
$ ss
Kali Def [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
12/17-09:34:21.777342 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54052 → 192.168.56.110:22
12/17-09:34:21.877167 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54053 → 192.168.56.110:22
12/17-09:34:21.980598 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54054 → 192.168.56.110:22
12/17-09:34:22.082569 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54055 → 192.168.56.110:22
12/17-09:34:22.181998 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54056 → 192.168.56.110:22
12/17-09:34:22.284725 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54057 → 192.168.56.110:22
12/17-09:34:22.310308 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.56.110
12/17-09:34:22.310351 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:34:22.335585 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.56.110
12/17-09:34:22.335622 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:34:22.361774 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:34:22.413998 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54066 → 192.168.56.110:22
12/17-09:34:22.439230 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.439230 [**] [116:420:1] "(tcp) TCP SYN with FIN" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22